UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)	)	**FILED UNDER SEAL**

APPLICATION OF THE UNITED STATES
FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)

The United States of America, moving by and through its undersigned counsel, respectfully submits under seal this *ex parte* application for an Order pursuant to 18 U.S.C. § 2703(d). The proposed Order would require CloudFlare, Inc., an Internet Service Provider located in San Francisco, California, to disclose certain records and other information pertaining to the CloudFlare, Inc. accountholders associated with the domains **ssndob.cc** and **ssndob.so**, described in Part I of Attachment A to the proposed Order filed herewith. The records and other information to be disclosed are described in Part II of Attachment A to the proposed Order. In support of this application, the United States asserts:

LEGAL BACKGROUND

1. CloudFlare, Inc. is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15) and/or a remote computing service as defined in 18 U.S.C. § 2711(2). Accordingly, the United States may use a Court Order issued under 18 U.S.C. § 2703(d) to require CloudFlare, Inc. to disclose the items described in Part II of Attachment A, as these records pertain to a subscriber of electronic communications or remote computing service and

are not the contents of communications. *See* 18 U.S.C. § 2703(c)(2) (Part II.A of Attachment A); . *See* 18 U.S.C. § 2703(c)(1) (Part II.B of Attachment A).

2. This Court has jurisdiction to issue the proposed Order because it is "a court of competent jurisdiction," as defined in 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(d). Specifically, the Court is a District Court of the United States that has jurisdiction over the offenses being investigated. *See* 18 U.S.C. § 2711(3)(A)(i).

3. A Court Order under § 2703(d) "shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Accordingly, the next sections of this application set forth specific and articulable facts showing that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation.

BACKGROUND

4. CloudFlare, Inc. is an internet service provider. It is a pay service that claims to "protect and accelerate websites." CloudFlare, Inc. offers to optimize and protect websites from unwanted web traffic and offer a full range of analytical data. CloudFlare, Inc. does not directly host or store website data but serves as a pass-through.

5. A network WHOIS search is a mechanism, or protocol, by which an investigator can query where a website, or other resource, is physically located, or by whom it is hosted. The resulting information from a WHOIS search includes, in the ordinary course, the location of the server or computer that is actually hosting the website.

6. CloudFlare, Inc.'s service can distort, or mask, the network WHOIS search protocol. As a result of CloudFlare's actions, a network WHOIS query of a customer of CloudFlare, Inc. results in it appearing as if the website is hosted by CloudFlare, Inc. when in reality it only serves as a pass-through. This effectively hides the location of the actual server.

THE RELEVANT FACTS

7. The United States Secret Service (USSS) is investigating known and unknown subjects operating a website, that illegally sells personally identifiable information (PII), such as dates of birth and social security numbers, known as **ssndob.cc** and **ssndob.so** for violations of Title 18 United States Code, Sections 1028A (aggravated identity theft); 1029 (access device fraud); 1030 (computer fraud); 1343 (wire fraud); 1956 (money laundering); and 371 & 1349 (conspiracy).

8. Customers of **ssndob.cc** and **ssndob.so** simply register a user name and password for the two aforementioned websites and are then able to access the websites and immediately query anyone residing in the United States by typing in the person's full name and the state in which the person whose name they have typed resides. The user is then able to purchase the social security number and date of birth of anyone they searched. Presently, the price for this information is $3.70 per social security number and date of birth combination. For the most part, the PII on these websites comes from data brokers or data aggregators whose computer systems were hacked and the PII is available to be queried; the computer systems on which the PII legitimately resides do not authorize the access of the PII in this way and are not aware it is being taken. Customers to these websites are able to pay by purchasing store credit through sending a wire or making an electronic currency transaction such as Bitcoin and/or WebMoney.

9. On September 12, 2014, an Undercover agent purchased the PII of approximately 10 US citizens. The purchased PII included each person's full name, current address, previous addresses, social security number and date of birth from **ssndob.so and ssndob.cc**. The Undercover agent advised that the domains **ssndob.so** and **ssndob.cc** both resolve to **ssndob.so.** The Undercover agent queried individuals by typing their full name and state of residence into a search field on the website. Based on open search queries and the investigator's personal knowledge, the information purchased belonged to each searched individual.

10. The USSS has investigated other such PII brokers and has learned that the customers of such PII use it to engage in numerous crimes, including wire fraud, bank fraud, credit card fraud, identity theft and the filing of fraudulent IRS tax returns claiming refunds in the names of innocent taxpayers whose PII is used.

11. A public internet WHOIS search of the domain **ssndob.cc** identifies the domain registration date as June 8, 2012. The WHOIS hosting value lists CloudFlare, Inc. in the location where the webhoster is generally located. CloudFlare, Inc. does not provide webhosting services. It is likely that CloudFlare, Inc. is serving as a pass-through service for the website **ssndob.cc**, for the apparent purpose of hiding the true location of the websites thereby making it more difficult for law enforcement to locate them. CloudFlare, Inc. will also likely have records reflecting who the true webhoster for **ssndob.cc** is, and will be able to provided account records for the subject who opened the CloudFlare service fo**r ssndob.cc**. Those records will assist the USSS in identifying and locating the person or persons who are managing **ssndob.cc**.

12. Included in the records that CloudFlare is likely to maintain are "A Records." "A records" map a FQDN (fully qualified domain name) to an IP address. This is usually the most often used record type in any Domain Name Service (DNS) system, which maps domain names

to IP addresses.

REQUEST FOR ORDER

13. The facts set forth in the previous sections show that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A to the proposed Order are relevant and material to an ongoing criminal investigation. Specifically, these items will help the United States to identify and locate the individual(s) who are responsible for the crimes described above and to determine other means of communication related to the commission of the Specified Federal offenses. Accordingly, the United States requests that CloudFlare, Inc. be directed to produce all items described in Part II of Attachment A to the proposed Order. Specifically, this Order requests the disclosure of the "A records" for the aforementioned domains, which map a FQDN to an IP address. This is usually the most often used record type in any DNS system that maps domain names to IP addresses.

14. The United States further requests that the Order require CloudFlare, Inc. not to notify any person, including the subscribers or customers of the account(s) listed in Part I of Attachment A, of the existence of the Order until further order of the Court. *See* 18 U.S.C. § 2705(b). This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." *Id.* In this case, such an Order would be appropriate because notification of the existence of the application and/or Order will result in one or more of the adverse circumstances listed in 18 U.S.C. § 2705(b), such as continued flight from prosecution, change patterns of behavior, or notify confederates. *See* 18 U.S.C. § 2705(b). In the experience of the USSS, if individuals who are engaged in this type of

illegal conduct become aware that law enforcement is attempting to track them they will destroy evidence, move the location of the website, and will otherwise attempt obstruct justice and avoid apprehension.

September 22, 2014.

Respectfully submitted,

JOHN KACAVAS
UNITED STATES ATTORNEY

/s/ Arnold H. Huftalen
Arnold H. Huftalen
Assistant United States Attorney